Insight 18 December 2024 | 21 min read

AI Watch: Global regulatory tracker - United States

The US relies on existing federal laws and guidelines to regulate AI but aims to introduce AI legislation and a federal regulation authority. Until then, developers and deployers of AI systems will operate in an increasing patchwork of state and local laws, underscoring challenges to ensure compliance.

Laws/Regulations directly regulating AI (the "AI Regulations")

Currently, there is no comprehensive federal legislation or regulations in the US that regulate the development of AI or specifically prohibit or restrict their use. That said, there are more than 120 AI bills being considered by the US Congress, covering a wide range of issues such as AI education, copyright disclosure, AI robocalls, biological risks, and AI's role in national security, including prohibiting AI from launching nuclear weapons autonomously.[1] Notably, many of the proposed bills emphasize the development of voluntary guidelines and best practices for AI systems, reflecting a cautious approach to regulation aimed at fostering innovation without imposing strict mandates. This approach is influenced by concerns over stifling technological progress and maintaining competitiveness, particularly against countries like China (which produces approximately four STEM graduates for every STEM graduate in the US). Given political divisions in the US and the influence of corporate lobbying, most of these bills are unlikely to become law.

Existing US federal laws have limited application to AI. A non-exhaustive list of key examples includes:

- Federal Aviation Administration Reauthorization Act, which includes language requiring review of AI in aviation.[2]

- National Defense Authorization Act for Fiscal Year 2019, which directed the Department of Defense to undertake various AI-related activities, including appointing a coordinator to oversee AI activities.[3]

- National AI Initiative Act of 2020, which focused on expanding AI research and development and created the National Artificial Intelligence Initiative Office that is responsible for "overseeing and implementing the US national AI strategy."[4]

Nevertheless, various frameworks and guidelines exist to guide the regulation of AI, including:

- The White House Executive Order on AI (titled Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence) which is aimed at numerous sectors, and is premised on the understanding that "[h]arnessing AI for good and realizing its myriad benefits requires mitigating its substantial risks."[5] The executive order focuses on federal agencies and developers of foundation models, mandates the development of federal standards, and requires developers of the most powerful AI systems to share safety tests results and other critical information with the U.S. government. The Executive Order also calls on the Department of Commerce to issue guidance for content authentication and watermarking to label AI-generated content. Note, the incoming Trump Administration has indicated plans to revoke this Executive Order.

- The White House Blueprint for an AI Bill of Rights, which asserts guidance around equitable access and use of AI systems.[6] The AI Bill of Rights provides five principles and associated practices to help guide the design, use and deployment of "automated systems" including safe and effective systems; algorithmic discrimination and protection; data privacy; notice and explanation; and human alternatives, consideration and fallbacks

- Several leading AI companies – including Adobe, Amazon, Anthropic, Cohere, Google, IBM, Inflection, Meta, Microsoft, Nvidia, Open AI, Palantir, Salesforce, Scale AI, Stability AI – have voluntarily committed to "help move toward safe, secure, and transparent development of AI technology."[7] These companies committed to internal/external security testing of AI systems before release, sharing information on managing AI risks and investing in safeguards.

- The Federal Communications Commission issued a declaratory ruling stating that the restrictions on the use of "artificial or pre-recorded voice" messages in the 1990s era Telephone Consumer Protection Act include AI technologies that generate human voices, demonstrating that regulatory agencies will apply existing law to AI.[8]

- The Federal Trade Commission (FTC) has also signaled an aggressive approach to use its existing authority to regulate AI.[9] The FTC recently issued a warning to market participants that it may violate the FTC Act to use AI tools that have discriminatory impacts, make claims about AI that are not substantiated, or to deploy AI before taking steps to assess and mitigate risks.[10] The FTC has already taken enforcement action against various companies that have deceived or otherwise harmed consumers through AI.[11] As discussed below, the FTC has notably banned Rite Aid from using AI facial recognition technology without reasonable safeguards.[12]

Status of AI-specific legislation

On September 12, 2023, the US Senate held public hearings regarding AI[13], which laid out potential forthcoming AI regulations. Possible legislation could include requiring licensing and creating a new federal regulatory agency. Additionally, US lawmakers held closed-door listening sessions with AI developers, technology leaders and civil society groups on September 13, 2023 in a continued push to understand and address AI.[14]

There are several federal proposed laws related to AI. A non-exhaustive list of key examples includes:

- The SAFE Innovation AI Framework,[15] which is a bipartisan set of guidelines for AI developers, companies and policymakers. This is not a law, but rather a set of principles to encourage federal law-making on AI.
- The REAL Political Advertisements Act,[16] which aims to regulate generative AI in political advertisements.
- The Stop Spying Bosses Act,[17] which aims to regulate employers surveilling employees with machine learning and AI techniques.
- The Draft No FAKES Act,[18] which would protect voice and visual likenesses of individuals from unauthorized recreations from Generative AI.
- The AI Research Innovation and Accountability Act,[19] which calls for greater transparency, accountability and security in AI, while establishing a framework for AI innovation. It would create an enforceable testing and evaluation standard for high-risk AI systems and require companies that use high-risk AI systems to produce transparency reports. It also empowers the National Institute of Standards and Technology to issue sector-specific recommendations to regulate them.

- The American Privacy Rights Act, which would create a comprehensive consumer privacy framework.[20] The draft bill includes provisions on algorithms, including a right to opt-out of covered algorithms used to make or facilitate consequential decisions.

State legislatures have also introduced a substantial number of bills aimed at regulating AI, notably:

- On May 17, 2024, Colorado enacted the first comprehensive US AI legislation, the Colorado AI Act. The Act creates duties for developers and for those that deploy AI. Unlike certain state privacy laws, there is no revenue threshold for applicability – the Act applies to all developers and deployers of high-risk AI systems in Colorado. The Act focuses on automated decision-making systems and defines a covered high-risk AI system as one that "when deployed, makes, or is a substantial factor in making a consequential decision" that has a material legal or similarly significant effect on the provision or denial to any consumer of, or the cost or terms of: education, employment, essential government services, healthcare, housing, insurance, and legal services. There is a specific focus on bias and discrimination, and developer and deployers must use reasonable care to avoid discrimination via AI systems that make, or are a substantial factor in making a consequential decision in the above enumerated fields. The Act will go into effect in 2026.

- In September 2024, California enacted various AI bills (many of which enter into force on January 1, 2025) relating to transparency, privacy, entertainment, election integrity, and government accountability. Some of the key laws include:
  - Assembly Bill 2655: Defending Democracy from Deepfake Deception Act[21]: requires large online platforms to identify and block the publication of materially deceptive content related to elections in California during specified time periods before and after an election. Additionally, under this Act, large online platforms must label – within 72 hours of notice – certain content as inauthentic, fake, or false during specified time periods before and after an election in California.
  - Assembly Bill 1836: Use of Likeness: Digital Replica Act[22]: establishes a cause of action for beneficiaries of deceased celebrities to recover damages for the unauthorized use of an AI-created digital replica of the celebrity in audiovisual works or sound recordings. This Act requires deployers of AI systems to obtain the consent of a deceased personality's estate before producing, distributing, or making available the digital replica of a deceased personality's voice or likeness in an expressive audiovisual work or sound recording.
  - Senate Bill 942: California AI Transparency Act[23]: mandates that "Covered Providers" (AI systems that are publicly accessible within California with more than one million monthly visitors or users) implement comprehensive measures to disclose when content has been generated or modified by AI. This Act outlines requirements for AI detection tools and content disclosures, and establishes licensing practices to ensure that only compliant AI systems are permitted for public use. Covered Providers that violate the Act are liable for a penalty of US$5,000 per violation per day.
  - Assembly Bill 2013: Generative AI: Training Data Transparency Act[24]: mandates that developers of generative AI systems (GenAI) publish a "high-level summary" of the datasets used to develop and train GenAI systems. For example, developers of GenAI systems would need to publish a summary of the following information, which is non-exhaustive:
    - Sources and owners of the datasets
    - Description of how the datasets further the intended purpose of the GenAI system
    - Whether the datasets include any information protected by IP law
    - Whether the datasets include personal information as defined in the CCPA
    - Whether the datasets were purchased or licensed by the developer

- Assembly Bill 3030: Health Care Services: Artificial Intelligence Act:[25] requires health care providers that use GenAI to generate patient communications to (i) disclaim that the communication was generated by a GenAI system, and (ii) provide clear instructions for how the patient can contact a human health care provider for assistance. Where the GenAI communication has been reviewed by a human health care provider, the disclaimer requirements do not apply.
- Other bills governing AI across a range of fields include:
  - Assembly Bill 2602: Contracts against Public Policy: Personal or Professional Services: Digital Replica Act[26]
  - Bill 896: Generative Artificial Intelligence Accountability Act[27]
  - Assembly Bill 2885: Unified Definition of Artificial Intelligence
- (Vetoed) Senate Bill 1047: Safe and Secure Innovation for Frontier Artificial Intelligence Models Act[28] The California Consumer Privacy Act,[29] which contains provisions on the use of automated decision-making tools. Additionally, the California Privacy Protection Agency released draft rules on these provisions[30] governing consumer notice, access and opt-out rights with respect to automated decision-making technology, which the rules define broadly. The regulations are still being finalized but will likely cover expanded uses of AI. The draft rules, which are still being formalized, would require significant disclosure about businesses' implementation and use of ADMT.

- In May 2024, the Utah Artificial Intelligence Policy Act[31] went into effect. The Act requires individuals and entities to disclose the use of GenAI in communications with consumers.
  - For individuals and entities that engage in "regulated occupations" (i.e., those who must obtain a license or state certification to practice the occupation, such as lawyers or health care providers), the disclosure must be made "prominently" at the beginning of any communication with the consumer, regardless of whether the consumer asks whether they are dealing with a GenAI system (i.e., a proactive disclosure obligation).
  - For individuals and entities that do not engage in "regulated occupations," the disclosure must be made "clearly and conspicuously" only if the consumer asks whether they are dealing with a GenAI system (i.e., a reactive disclosure obligation).
  - Non-compliant individuals and entities may be fined up to US$2,500 per violation by the Utah Division of Consumer Protection.
  - Enactment of the Utah Artificial Policy Act and the California Health Care Services: Artificial Intelligence Act both underscore legislative concern with ensuring that consumers know when they are dealing with GenAI systems in certain settings.
- More than 40 state AI bills were introduced in 2023, with Connecticut[32] and Texas[33] actually adopting statutes. Both of those enacted statutes establish state working groups to assess state agencies' use of AI systems to ensure they do not result in unlawful discrimination.

As for international commitments, on September 5, 2024, the United States joined Andorra, Georgia, Iceland, Norway, the Republic of Moldova, San Marino, the United Kingdom, Israel, and the European Union to sign the Council of Europe's Framework Convention[34] on AI. The treaty will enter into force on the first day of the month following three months after five signatories, including at least three Council of Europe Member States, have ratified it. Countries from all over the world will be eligible to join and commit to its provisions.

Other laws affecting AI

Existing legislation has been the primary way in which the US regulates AI as established law, including privacy and intellectual property laws, which are generally applicable to AI technologies.

Notably, in April 2023, the Federal Trade Commission, Equal Employment Opportunity Commission, Consumer Financial Protection Bureau, and Department of Justice issued a joint statement noting that "existing legal authorities apply to the use of automated systems and innovative new technologies."[35] As cited above, in February 2024, the Federal Communications Commission applied restrictions in the Telephone Consumer Protection Act on AI-generated voices.

Several states have enacted comprehensive privacy legislation that can also regulate AI. A non-exhaustive list of notable state legislation includes:

- The California Privacy Protection Act (CPPA), which regulates automated decision-making[36]
- The Biometric Information Privacy Act in Illinois,[37] which is very broad and allows for extremely high damages for violations. There is currently pending litigation in the AI context

Existing intellectual property laws also apply to AI, both with respect to the data AI technologies are trained upon and the outputs of such technologies. For example, with respect to outputs, the US District Court has held that human authorship is an essential part of a valid copyright claim, and the Copyright Office will refuse to register a work unless it was created by a human being."[38] There are also numerous cases before the courts in the US alleging copyright infringement, among other things, with respect to training data.

Definition of "AI"

There is no single definition of AI.

The National Artificial Intelligence Initiative and White House Executive Order on AI define AI as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action."[39]

Many state privacy bills have different definitions of automated decision-making technology or "profiling":

- A recent Texas statute establishing an AI advisory council (HB 2060) defines an "automated decision system" as "an algorithm, including an algorithm incorporating machine learning or other artificial intelligence techniques, that uses data-based analytics to make or support governmental decisions, judgments or conclusions"[40]

- Connecticut's Public Act No. 22-15 defines "profiling" as "any form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements" [41]

- The CCPA defines "profiling" as "any form of automated processing of personal information, [...] to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements."[42]

  - Additionally, recently enacted California Assembly Bill 1008[43] clarifies that the CCPA applies to consumers' "personal information" regardless of its format. Specifically, AB 1008 clarifies that the CCPA encompasses "personal information" contained in "abstract digital formats" (i.e., generative AI systems that are capable of outputting consumers' personal information).

  - Further, recently enacted California Senate Bill 1223[44] clarifies that "sensitive personal information" under the California Privacy Rights Act (CPRA) encompasses consumers' neural data. As with AB 1008, SB 1223 aims to keep pace with emerging technology (in this case, neurotechnology) in an effort to protect information about consumers' brain and nervous system functions. While SB 1223 does not articulate a specific nexus to AI systems, if signed into law, it would constrain developers and deployers from using neural data under the CPRA.

Territorial scope

As noted above, there are currently no comprehensive federal laws that have been enacted to specifically regulate AI. Accordingly, there is no specific territorial scope of federal legislation. However, many existing statutes regulate activities in which AI can be used, and those federal statutes typically apply nationally and, in some cases, extra-territorially. State legislation regulating AI generally has extra-territorial effect as its application typically extends to entities that target its residents from within or outside the state.

Sectoral scope

As noted above, there are currently no comprehensive federal laws that directly regulate AI. Accordingly, there is no specific federal sectoral scope at this stage. Nevertheless, there are certain sector-specific frameworks that have been implemented in the US to regulate the use of AI. A non-exhaustive list of key examples includes:

- In the insurance sector, the National Association of Insurance Commissioners issued a model bulletin[45] that focuses on governance frameworks, risk management protocols and testing methodologies that insurers should have in place to govern their use of AI systems that impact insurance consumers. Once adopted by the NAIC (expected early 2024), state insurance departments could use the bulletin at their discretion as the bulletin is not new law, but instead enforces the application of current laws to insurers' use of AI and serves as guidance as to regulatory expectations
- In the employment sector, the City of New York enacted Local Law 144 of 2021[46] that "prohibits employers and employment agencies [in the city] from using an automated employment decision tool unless the tool has been subject to a bias audit within one year of the use of the tool, information about the bias audit is publicly available, and certain notices have been provided to employees or job candidates"[47]

Compliance roles

As noted above, there is currently no comprehensive federal legislation in the US that directly regulates AI. Accordingly, there are currently no specific or unique federal obligations imposed on developers, users, operators and/or deployers of AI systems. However, developers, users, operators and deployers of AI systems should anticipate that existing law will apply to any regulated activity that uses AI, and consult legal counsel about the potential liabilities that may arise. While potentially novel, the use of AI does not per se provide a shield from the application of existing law.

Core issues that the AI regulations seek to address

As noted above, there is currently no comprehensive legislation in the US that directly regulates AI. However, the White House Executive Order on AI and proposed legislation at the federal and state level generally seeks to address the following issues:

- Safety and security

- Responsible innovation and development
- Equity and unlawful discrimination
- Protection of privacy and civil liberties

Risk categorization

As noted above, there is currently no comprehensive legislation in the US that directly regulates AI. AI is also not generally classified according to risk in the relevant frameworks and principles.

Key compliance requirements

As noted above, there is currently no comprehensive federal legislation in the US that directly regulates AI. Nevertheless, the White House Executive Order on AI lists the following eight key principles and priorities to encourage the responsible development of AI technologies and safeguard against potential harms:

- AI must be safe and secure
- To lead in AI, the US must promote responsible innovation, competition and collaboration
- Responsible development and use of AI requires a commitment to supporting American workers
- AI policies must advance equity and civil rights
- The interests of Americans who increasingly use, interact with, or purchase AI and AI-enabled products in their daily lives must be protected
- Privacy and civil liberties must be protected
- The federal government must manage the risks of its own use of AI
- The federal government should exercise global leadership in societal, economic and technological progress[48]

Regulators

Currently, there is no AI-specific federal regulator in the US. However, in April 2023, the Federal Trade Commission, Equal Employment Opportunity Commission, Consumer Financial Protection Bureau and Department of Justice issued a joint statement clarifying that their authority applies to "software and algorithmic processes, including AI."[49]

Similarly, state regulators that regulate privacy legislation likely also have the authority to regulate AI vis-à-vis existing privacy provisions. The FTC has been active in this area, and we can expect to see more from them going forward; see discussion of Rite Aid below.

Enforcement powers and penalties

As noted above, there are currently no comprehensive federal laws or regulations in the US that have been enacted specifically to regulate AI. As such, enforcement and penalties relating to the creation, dissemination and/or use of AI are governed by application of existing law to situations involving AI, through regulatory or judicial application of non-AI-specific federal and state statutes or AI-specific state privacy legislation.

In addition, the Federal Trade Commission has evoked an interest in and focus on regulating AI through enforcement. On December 19, 2023, the FTC settled a significant action focused on artificial intelligence bias and discrimination against Rite Aid regarding the company's use of facial recognition technology for retail theft deterrence. This illustrative case provides guidance on the FTC's enforcement on AI systems. For example, the proposed consent order[50] between Rite Aid and the FTC:

- Prohibits Rite Aid from using AI facial recognition for five years
- Requires Rite Aid to delete all photos and videos of consumers used in its AI facial recognition
- Specifies that after Rite Aid's ban on using AI facial recognition expires, if Rite Aid operates AI facial recognition technology for surveillance, it must maintain a comprehensive automated biometric security or surveillance system monitoring program that identifies and addresses the risks of such operation and notifies consumers of its use of AI facial recognition. Rite Aid must also provide a means for consumers to lodge complaints, and investigate and respond to all complaints received, among other requirements

With respect to Colorado AI Act, the Colorado Attorney General has rule-making authority to implement, and exclusive authority to enforce, the requirements of the Act.[51] A developer or deployer who violates the Act is deemed to engage in unfair or deceptive trade practices.

Enforcement mechanisms and penalties vary under the different California AI bills. Bills that specifically provide for enforcement include:

- Senate Bill 942: California AI Transparency Act: provides for penalties of US$5,000 per violation per day, enforceable through civil action by the California Attorney General, city attorneys, or county counsel
- Assembly Bill 3030: Health Care Services: Artificial Intelligence Act: enforceable by the Medical Board of California and Osteopathic Medical Board of California, with non-compliance punishable by, inter alia, civil penalties, suspension or revocation of a medical license, and administrative fines as set out in the California Health and Safety Code
- Assembly Bill 2655: Defending Democracy from Deepfake Deception Act: the California Attorney General, any district attorney, or any city attorney may seek injunctive relief to compel removal of materially deceptive content

Further insights from White & Case:

- SEC Will Prioritize AI, Cybersecurity, and Crypto in its 2025 Examination Priorities
- NYDFS Releases Artificial Intelligence Cybersecurity Guidance For Covered Entities
- Raft of California AI Legislation Adds to Growing Patchwork of US Regulation
- Newly passed Colorado AI Act will impose obligations on developers and deployers of high-risk AI systems
- Long awaited EU AI Act becomes law after publication in the EU's Official Journal (July 2024)
- Dawn of the EU's AI Act: political agreement reached on world's first comprehensive horizontal AI regulation
- Processing personal data using AI Systems (Part 1)
- The EU AI Act's extraterritorial scope (Part 2)

Nick Reem (Associate, White & Case, Los Angeles) contributed to this publication.

1 See MIT Technology Review article

2 See Federal Aviation Administration Reauthorization Act

3 See National Defense Authorization Act

4 See National AI Initiative Act of 2020

5 See White House Executive Order on AI

6 See White House Blueprint for an AI Bill of Rights

7 See White House fact sheet

8 See FCC declaratory ruling

9 See EEOC-CRT-FTC-CFPB-AI-Joint-Statement (final)

10 See Keep your AI claims in check

11 See FTC Announces Crackdown on Deceptive AI Claims and Schemes

12 See Rite Aid Banned from Using AI Facial Recognition

13 See The Need for Transparency in Artificial Intelligence

14 See IAPP article

15 See SAFE Innovation AI Framework

16 See REAL Political Advertisements Act

17 See Stop Spying Bosses Act

18 See NO FAKES Act

19 See AI Research, Innovation, and Accountability Act

20 See American Privacy Rights Act

21 See Defending Democracy from Deepfake Deception Act

22 See Use of likeness: digital replica

23 See California AI Transparency Act

24 See Bill Text- AB-2013 Generative artificial intelligence: training data transparency

25 See Bill Text- AB-3030 Health care services: artificial intelligence

26 See Bill Text- AB-2602 Contracts against public policy: personal or professional services: digital replicas

27 See Generative Artificial Intelligence Accountability Act

28 See Safe and Secure Innovation for Frontier Artificial Intelligence Models Act

29 See California Consumer Privacy Act

30 See Draft Automated Decision-making Technology Regulations

31 See Utah S.B. 149 Artificial Amendments

32 See An Act concerning AI, automated decision-making and personal data privacy

33 See An Act relating to the creation of the AI council

34 See Convention text here

35 See EEOC-CRT-FTC-CFPB-AI-Joint-Statement

36 See California Consumer Privacy Act of 2018

37 See 740 ILCS 14/ Biometric Information Privacy Act

38 See THALER v. PERLMUTTER

39 See here

40 See An Act relating to the creation of the AI council

41 See An Act concerning personal data privacy and online monitoring

42 See California Consumer Privacy Act of 2018

43 See California Consumer Privacy Act of 2018: personal information

44 See Consumer privacy: sensitive personal information: neural data

45 See Model- Innovation, Cybersecurity, and Technology (H) Working Group

46 See The New York City Council File

47 See DCWP- Automated Employment Decision Tools (AEDT)

48 See Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

49 See Joint Statement

40 See Stipulated Order For Permanent Injunction and Other Relief

51 See Colorado AI Act